REMARKS

Claims 1-5, and 7 were rejected under 35 USC § 103(a) as being unpatentable over Cornelius et al (US Pub. No. 2003/0165136) in view of Jade et al (US Pat. No. 5,944,823), and further in view of Berg et al (US Pat. No. 6,674,713). Claim 6 is rejected under 35 USC § 103(a) as being unpatentable over Cornelius in view of Jade, Berg, and further in view of Fan et al (US Pat. No. 6,219,706). Claims 8-9 and 12-18 were rejected under 35 USC § 103(a) as being unpatentable over Jade et al (US Pat. No. 5,944,823), in view of Cornelius et al (US Pub. No. 2003/0165136). Claims 10-11 were rejected under 35 USC § 103(a) as being unpatentable over Jade et al (US Pat. No. 5,944,823), in view of Cornelius et al (US Pub. No. 2003/0165136) and further in view of Berg et al (US Pat. No. 6,674,713). Claims 19-20 were rejected under 35 USC § 103(a) as being unpatentable over Jade et al (US Pat. No. 5,944,823), in view of Cornelius et al (US Pub. No. 2003/0165136).

Jade teaches that a "special tunneling mechanism" is needed to establish a connection through a firewall:

> The disclosed invention provides a **special "tunneling" mechanism**, operating on **both sides** of a **firewall**, for **establishing** such "outside in" **connections** when they are requested by certain "**trusted**" individuals or objects or **applications** outside the firewall. (Jade abstract, emphasis added)

The purpose of the "special tunneling mechanism" is to establish connections through the firewall for "trusted" applications.

This special tunneling mechanism is a special application required on both sides of the firewall. Each special tunneling application keeps a copy of a table of "trusted" sockets for the "trusted" applications:

> The mechanism includes **special tunneling applications, running** on interface servers **inside and outside the firewall**, and a special **table** of "trusted **sockets**" created and maintained by the inside tunneling application. (Jade abstract, emphasis added)

The table of "trusted sockets" contains entries for "trusted sockets" or connections for trusted applications. The "special tunneling application" opens or "establishes" these connections on behalf of these "trusted" applications.

Jade's "Control Connection" to Open Firewall Window Cannot Be Used for VoIP Data

The connection used to update the table of "trusted sockets" and open the firewall window is different from the connection window established for these "trusted" applications. Thus two very different connections are used by Jade:

1.) One connection is private and used only by the special tunneling application to control the opening or establishment of firewall windows. This first connection is known as the "control connection".

2.) The second connection is the connection between the trusted applications themselves. This connection corresponds to a "trusted socket" in the special table maintained by the special tunneling mechanism.

These 2 connections cannot be the same connection because this is specifically taught away by Jade:

> The inside interface server also establishes a "**control connection**" to an outside interface server which interfaces between the firewall and all objects outside the firewall. The control connection is **accessible only** to the **tunneling application** running on the inside interface server and a corresponding tunneling application running on the outside interface server; i.e. it is **not directly accessible to any other applications** running on these interfaces servers, and is **totally inaccessible** to both inside and outside objects not residing on these servers. (Jade col 2, lines 13-22, emphasis added)

Jade thus teaches that these 2 connections are separate. Indeed, Jade teaches that other applications cannot use the "control connection":

> The control connection is **accessible only** to the **tunneling application** running on the inside interface server and a corresponding tunneling application running on the outside interface server; i.e. it is **not directly accessible to any other applications** running on these interfaces servers, and is **totally inaccessible** to both inside and outside objects not residing on these servers. (Jade col 2, lines 16-22, emphasis added)

Since "any other applications" would include the "trusted" applications that the "special tunneling applications" created a firewall window for, (by listing them as a "trusted" application with a "trusted socket" in the special table), the "trusted" applications cannot use the "control connection" Any packets sent over this "control connection" would be **"totally inaccessible"** to all other applications, including the "trusted" applications or any VoIP application.

Claims recite Same Connection for both Opening Firewall and Sending User Data

On page 3 of the office action, Jade was cited for teaching packet transmission to open the firewall hole: "Jade discloses opening a hole in the firewall through packet transmission (see for example; col 4 ln 25-39)." Since Jade's packets to open or establish a firewall hole or "trusted socket" would go through his "control connection" which is **"totally inaccessible"** to all other applications, Jade's packets cannot be used for both opening the firewall and for sending user data.

Jade must use one set of packets over his "control connection" to open the firewall. Jade opens the firewall window by updating the "trusted sockets" in his tables. Another set of user-data packets is then sent over the "trusted socket" connection.

Jade's user-data packets cannot be sent through his "control connection" because Jade specifically states that the "control connection" is **not directly accessible to any other applications** running on these interfaces servers, and is **totally inaccessible**" (Jade col 2, lines 18-22, emphasis added).

In contrast, claim 1 recites that the same firewall window is used both to open the window and for user data. Claim 1's "null-packet generator" recites that the null packet that opens the firewall is sent from the "local UDP port" through the firewall:

> sending the null UDP packet from a local UDP port through the local firewall toward the remote client

In response to this packet, the

> local firewall opens a window between the local UDP port and the remote UDP port in response to the null UDP packet

This same firewall window is then used for user data carried by other UDP packets:

> receiving **UDP packets** containing **user data** from the remote client **through** the **window** in the local firewall

Thus both the firewall-opening packet (the "null UDP packet"), and the additional "UDP packets" of "user data" pass through the **same** window in the firewall.

In contrast, Jade teaches that information to open the window (updates for entries in the table of trusted sockets) is sent through his "control connection" (col 3, lines 40-43). Packets of application data are then sent through other connections that correspond to "trusted sockets" listed in his table. Application-data packets are **not** sent through the "control connection".

Thus Jade teaches that different connections are needed for use by the "special tunneling" application to set up windows, and by other "trusted" applications that use these windows rather than the control connection. The prior-art using 2 different connections, rather than a single connection, is an indication of non-obviousness.

Jade alone or in combination with the other reference cannot teach or suggest that the same window (identified by the local UPD port and remote UDP port) is used for both opening that window and user data sent through that window. Jade teaches away since Jade uses a different "control connection" to open a window. The "control connection" and the window opened are different connections.

Claim 7 further recites that the firewall window is used for audio or video data:

> the window in the local firewall is used for a two-way direct communication channel between the local UDP port of the local client, and the remote UDP port of the remote client, wherein UDP packets containing audio or video data are transmitted in two directions between the remote and local clients through the window in the local firewall

Jade teaches that other "trusted" applications (such as an audio-data application) use "trusted sockets" and cannot use the "control connection" which is "**totally inaccessible**".

Claim 19's Firewall-Opening Packet uses same Window, Jade uses different Connections

Independent claim 19 recites a "firewall-opening packet means" that generates "a firewall-opening packet". This firewall-opening packet "is destined to the remote UDP port of the remote peer". The firewall-opening packet is specifically sent from the local UDP port to the remote UDP port:

> the network connection means also for sending the **firewall-opening packet from** a **local UDP port**, the firewall-opening packet **destined** for the **remote UDP port** of the remote peer;

Transmission of this firewall-opening packet through the firewall automatically opens the window in the firewall:

> wherein a **window** in the **firewall** is **created when** the **firewall-opening packet** is **sent**, the window allowing packets from the remote peer to reach the network connection means through the firewall;

The firewall window is thus established between the local and remote UDP ports. This same window, identified by the same "local UDP port" and "remote UDP port" is then used for direct communication:

> direct communication means, coupled to the network connection means, for **sending UDP packets from** the **local UDP port** to the **remote UDP port** of the remote peer **through** the **window** in the **firewall** created by the firewall-opening packet,

Claim 19 here recites that additional UDP packets are sent through this window to the remote UDP port.

Since the same "local UDP port" and "remote UDP port" are used by both the "firewall-opening packet" and the "UDP packets", Claim 19 recites that the same window is used both for opening the firewall window and for sending user data through that window. As noted above, Jade uses a "trusted socket" that is separate from his "control connection".

Cornelius teaches Manual Firewall Opening, Cannot be Combined with Jade

Cornelius cannot fairly be combined with the automated firewall-opening mechanism of Jade because Cornelius explicitly teaches that a human "system administrator" manually configures the firewall:

> Essentially, the firewall closes the ports for incoming traffic unless **someone** (e.g., the administrator of the firewall) can vouch that the destination port has a trusted program digesting the information. (Cornelius para. [0012], emphasis added)

Cornelius recognizes the workload burden this places on that "someone", the system administrator:

> With RTP, the ports are 'unspecified', so the **administrator could end up** with **having** to **open up many**, or **all** of the **UDP ports** to allow the voice traffic to come in. (Cornelius para. [0012], emphasis added)

This "someone" has to configure the firewall to allow the VoIP packets to pass through:

> This destination port number is provided to the **administrator** of the firewall **who** then **configures** the **firewall** to allow incoming RTP data traffic through to the designated destination UDP port number. (Cornelius para. [0039], emphasis added)

Configuration requires that the system administrator enter port numbers into databases to create the hole in the firewall:

> For example, a **port number** could be set in a configuration **database** 37A, . . . 37L, . . . 37N, 38 at the time the **hole** is **inserted** in the **firewall by** the **system administrator**. (Cornelius para. [0038], emphasis added)

Cornelius emphasizes that databases have to be updated "manually" with information by the system administrator:

> This information is entered into the system **manually** by the system administrator or **someone** similar who uses the management interface in the telephony management system (TMS) to add the new PBX. (Cornelius para. [0046], emphasis added)

Other persons are not allowed to open a firewall hole, only the system administrator:

> The firewall administrator is usually the **only one authorized** to open a hole at this chosen port number. (Cornelius para. [0055], emphasis added)

Proposed Combination Destroys Purpose of Cornelius Reference

Cornelius thus explicitly teaches that **someone**, a human **system administrator**, is needed to open the hole in the firewall. Indeed, the purpose of Cornelius is to "limit the number of holes a system administrator must open in a firewall" (abstract). This purpose would make no sense and be irrelevant if the proposed combination were made.

Proposed Combination Is Directly Contrary to Explicit Teaching of Reference

Indeed, the proposed combination of Cornelius with Jade not only destroys this stated purpose of Cornelius, but it also is contrary to the explicit teachings of Cornelius. Cornelius explicitly teaches that the firewall hole is "**manually**" opened by a human "**system administrator**". A proposed modification of a primary reference cannot ignore explicit teachings of the primary reference.

Explicit Teachings of Cornelius Teach Away from Proposed Modification

The combination of references as a whole includes the explicit teachings of the primary Cornelius reference, including teachings that explicitly teach away from the proposed modification. A proposed modification of the primary reference cannot be fairly made when it goes against so many explicit teachings in the primary reference.

The explicit teachings, cited above, inside the Cornelius reference explicitly teach that a human system administrator is required to open the firewall hole. Using another mechanism, such as Jade's "special tunneling mechanism" to open this firewall hole contradicts these explicit teachings of Cornelius and thus is not proper. An automated mechanism to open the firewall hole is the complete ***antithesis*** of the manual firewall configuration explicitly taught by Cornelius.

Berg's Null Segments Test Existing Connection, do not Establish New Connection

Neither Cornelius nor Jade teach null packets as the firewall-opening packet. Berg was cited as teaching null segments or packets. Berg teaches a NUL segment at col 22. lines 25-33. In particular,

> "The NUL segment is used to determine if the other side of a connection is **still active**." (Berg col 22, lines 26-27, emphasis added).

Berg teaches that null packets are used as keep-alive packets to see if the connection is still active. Being "still active" implies that the connection was "active" in the first place, **before** the null packet was sent.

It is not possible to "keep alive" something that was never alive in the first place !

In contrast, Applicant sends the null packet first, **before** there is any connection, to open the firewall window. Independent method claim 8 recites:

> sending the firewall-opening packet from the second computer toward the first computer;
> opening a window in a firewall that protects the second computer from receiving un-requested packets when the firewall-opening packet is sent by the second computer, the window allowing packets from the first computer to reach the second computer through the firewall; and
> sending direct communication packets from the first computer to the second computer through the window in the firewall created by the firewall-opening packet sent by the second computer in response to the message from the third computer,
> whereby the window in the firewall protecting the second computer is created for use by the first computer.

Claim 10 recites that this "firewall-opening packet" is a "null packet" having no data in a data payload.

Berg teaches that his NUL segment is used to determine if the connection is "still active". In contrast, Applicant sends the null or firewall-opening packet to open the window to allow other user-data packets to use the connection.

Applicant's null packet opens the window through the firewall that is otherwise blocking the connection from being established. Berg sends null segments to test if an existing connection is still active.

In view of the above, it is submitted that claims 1-20 are in a position for allowance. This application was filed with formal drawings. Applicant believes that a full and complete response to the office action has been made. Reconsideration and re-examination is respectfully requested. Allowance of the claims at an early date is solicited.

If the Examiner believes that a telephone interview would expedite prosecution of this application, he is invited to telephone the undersigned at (831) 476-5506.

Respectfully Submitted,

Stuart T. Auvinen
429 26th Avenue
Santa Cruz, CA 95062

(831) 476-5506
(831) 477-0703 Fax

Stuart T. Auvinen
Agent for Applicant
Reg. No. 36,435